Les enjeux immenses de l'innovation

Tendances des attaques ciblant les services financiers

À une époque marquée par une transformation digitale sans précédent, le secteur des services financiers se retrouve à la croisée de l'innovation et du risque. Alors que la technologie remodèle le paysage des transactions financières, elle ouvre, dans le même temps, une nouvelle ère de menaces qui ciblent la stabilité économique en plein cœur.

Attaques contre les services financiers et leurs clients

9 milliards

Nombre d'attaques d'applications Web et d'API contre les services financiers

Numéro 1

Le segment des services financiers est celui qui subit le plus d'attaques DDoS, dépassant même le secteur des jeux vidéo

50,6 %

Les services financiers ont connu le plus grand nombre de victimes d'attaques par hameçonnage au deuxième trimestre 2023

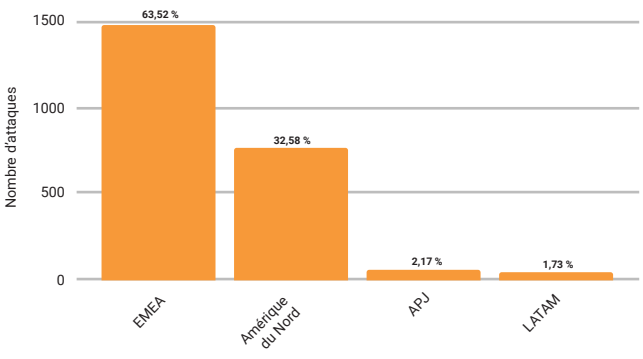
+ de 1 000 milliards

Nombre de requêtes de bots malveillants

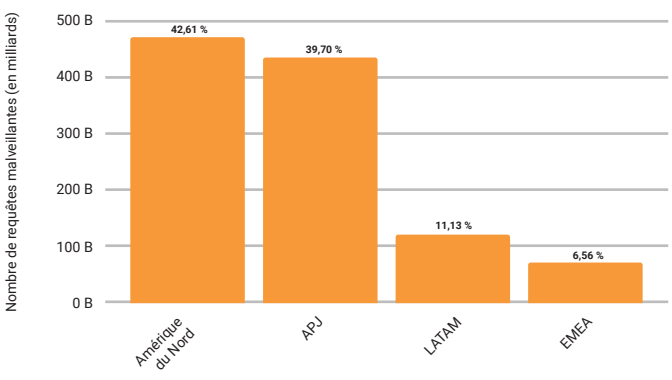
Situations régionales

Le nombre d'attaques DDoS de couche 3 et 4 en Europe, au Moyen-Orient et en Afrique (EMEA) est presque deux fois supérieur à celui observé en Amérique du Nord

Attaques DDoS par régions : services financiers
Du 1er janvier 2022 au 30 juin 2023



Requêtes de bots malveillants par région : services financiers
Du 1er janvier 2022 au 30 juin 2023



La région Asie-Pacifique et Japon (APJ) est la deuxième région la plus ciblée par les requêtes de bots malveillants

Risques de sécurité potentiels à surveiller

API fantômes

Les API non documentées et non suivies peuvent poser des problèmes de surveillance pour les entreprises qui ne savent pas qui utilise ces API et de quelle manière.

Scripts tiers

Les attaquants peuvent exploiter des vulnérabilités côté client ou injecter du code malveillant dans des scripts tiers chargés sur le site Web. Les services financiers sont ainsi exposés au web skimming, ce qui peut entraîner le vol des données de leurs clients ou leur utilisation dans des transactions non autorisées.

Agrégateurs financiers

Les failles de sécurité entre les agrégateurs financiers et la manière dont les données sont collectées peuvent potentiellement ouvrir une nouvelle voie pour les attaquants et mener à l'usurpation d'identité.

Recommandations en matière de sécurité et meilleures pratiques

- Comprenez votre surface d'attaque pour concevoir des stratégies d'atténuation et mettre en place des contrôles de sécurité.
- Déployez des outils de sécurité des API pour détecter et surveiller les API malveillantes.
- Utilisez la liste des 10 principaux risques pour la sécurité des API selon l'OWASP et l'infrastructure ATT&CK de MITRE pour développer des plans de formation et de test destinés à vos équipes rouges ou à vos groupes de test de pénétration.
- Utilisez une stratégie de défense à plusieurs niveaux, qui comprend la réalisation régulière d'audits de sécurité et la mise en œuvre d'une méthode de détection et d'atténuation avancée.
- Utilisez des solutions telles que Client-Side Protection & Compliance (anciennement Page Integrity Manager) qui peuvent atténuer les risques posés par les attaques côté client.
- Créez un modèle de gouvernance en bordure de l'Internet pour davantage de visibilité sur le trafic des bots/API.
- Menez un exercice en conditions réelles si vous n'avez pas subi d'attaque DDoS au cours des trois derniers trimestres. Validez vos plans d'action et suivez les tendances, tant en termes de taille que de vitesse, afin d'évaluer vos risques en fonction de vos capacités actuelles.

Pour en savoir plus sur les tendances en matière d'attaque dans le secteur des services financiers, lisez notre rapport complet.

Télécharger le rapport

 | Assistance | Publication : 10/23